

CCR MASTER EXTRACT POLICY

Updated May 2005

The following scenario depicts the process in which all DLIS CCR Master extracts will be handled.

TEN files (5 Refresh, 5 Daily) will be created and stored on a secured (User code/password) DLISCCR server in zipped format. These files will contain a complete listing of all current active records. Each file will store a different type of view, **For Official Use Only**, **Proprietary**, **Sensitive**, **MPIN**, and **Complete** data.

The daily file will contain only new and change records from the previous day. These files will stay on the server for 30 days.

The above allows for three types of processing to take place:

- Downloading of the monthly extract each month to refresh a user database.
- Download the monthly database once then by downloading the daily update files each day keeps the database in sync with DLIS.
- A combination of 1 and 2 where a complete refresh is done each month even though the daily updates were processed.

Each user will be assigned a UserId and Password allowing for access to the extract files on the DLISCCR Server. Each UserId will be assigned on an as needed basis for the type of data wanted. Each user that will access the CCR data will be required to sign a Non-Disclosure Agreement, which can be found at www.ccr.gov

It will be the users responsibility to pull the zipped extract files from the DLISCCR Server, unzip the extract files once downloaded and load said extract files to their database.

Access Limitations and Locations

To comply with the encryption requirements for sensitive CCR information, the transfer of this data will be performed in a secure manner.

The **For Official Use Only**, **Proprietary**, **Sensitive**, **MPIN**, and **Complete** extract can be accessed and downloaded through **FTP** at [ftp.bpn.gov](ftp://ftp.bpn.gov) (**updated October 2004)

SFTP FILE DIRECTORY

■ **DIR1/FOIA**

- **DIR2/PROPRIETARY**
- **DIR3/SENSITIVE**
- **DIR4_1/MPIN**
- **DIR4_2/COMPLETE**

The **For Official Use Only, Sensitive, Proprietary, MPIN, and Complete** extracts can be accessed and downloaded through the Web site https://ftp.bpn.gov/web_extracts using Microsoft Explorer (version 3 or greater).

Microsoft Explorer encrypts the user-id and password.

Once verification is complete the file transfer is done through SSL.

- **FOIA files are stored in Public Directory**
- **Proprietary files are stored in Proprietary Directory**
- **Sensitive files are stored in Sensitive Directory**
- **MPIN files are stored in MPIN Directory**
- **Complete files are stored in Complete Directory**

File Naming Conventions

Position #1 = 'C' to indicate 'CCR' file

Position #2 and #3 = file type (below)

Position #4 - #8 = Julian Date

- CR = Complete Refresh
- FR = For Official Use Only Refresh
- PR = Proprietary Refresh
- SR = Sensitive Refresh
- MR = MPIN Refresh
- CD = Complete Daily
- FD = For Official Use Only Daily
- PD = Proprietary Daily
- SD = Sensitive Daily
- MD = MPIN Daily

New monthly files are available on the last day of the month by 08:00.

Daily update files are produced Tuesday – Saturday and are available on the server by 08:00.

Point of Contact Information

CCR Program Management Office/Operations
Defense Logistics Information Services (DLIS)

Thresa Cameron/269-961-4385

Thresa.cameron@dla.mil

Peggy Lockwood/269-961-5574

Peggy.lockwood@dla.mil

Secure FTP details:

A DLA mandate effective Jan 2004: FTP is no longer available eliminating open FTP access to CCR Extract server as of 1/31/2003. SSH software is now required to connect via SSH/SFTP to the CCR Extract server using port 22. Use software appropriate commands and syntax. Batch connections require a public key authentication, contact server administrator for configuration/setup.

Customers who are DLA agencies with connecting machines are on DLA network can be given FTP access. Customer IP address is needed and setup will be done through DLIS security. This exception will not apply once CCR is implemented in ESE.